Building a better
working world

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Google Trust Services LLC and Google Trust Services Europe Limited:

Scope
We have examined the accompanying assertion made by the management of Google Trust Services LLC and Google Trust Services Europe Limited (collectively, GTS), titled *Management's Assertion Regarding the Effectiveness of Its Controls Over the S/MIME Certificate Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities – S/MIME, Version 1.0.3* that for its Certification Authority (CA) services at New York, USA, South Carolina, USA, Oklahoma USA, Ghlin, Belgium, and Zurich, Switzerland for CAs as enumerated in **Appendix A,** throughout the period from September 1, 2023 through August 31, 2024. GTS has:

Disclosed its S/MIME certificate lifecycle management business practices in the applicable versions of GTS' Certification Practice Statement ("CPS") and S/MIME Certificate Policy ("S/MIME CP") as referenced in **Appendix B**.

including its commitment to provide S/MIME Certificates in conformity with the applicable CA/Browser Forum Requirements on the GTS website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
    - S/MIME subscriber information is properly authenticated (for the registration activities performed by GTS)
- Maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

based on the *WebTrust Principles and Criteria for Certification Authorities – S/MIME, Version 1.0.3*.

Management's responsibilities
GTS' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the *WebTrust Principles and Criteria for Certification Authorities – S/MIME, v1.0.3*.

Our responsibilities
Our responsibility is to express an opinion on GTS management's assertion based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at GTS and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was not conducted for the purpose of evaluating GTS's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of GTS and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

Other matters
GTS' management has disclosed to us the attached matters referenced in **Appendix C** that the Company has posted publicly in the online forums of the CA/Browser Forum, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these matters in our risk assessment and in determining the nature, timing, and extent of our procedures.

Inherent limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, GTS may achieve reasonable, but not absolute assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are achieved. Controls may not prevent or detect and correct,

error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Further, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, letter that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

Opinion
In our opinion, GTS' management's assertion referred to above, is fairly stated, in all material respects, based on the aforementioned criteria.

This report does not include any representation as to the quality of GTS' CA services beyond those covered by the *WebTrust Principles and Criteria for Certification Authorities – S/MIME, Version 1.0.3*, or the suitability of any of GTS' services for any customer's intended purpose.

GTS' use of the WebTrust for Certification Authorities – S/MIME Seal constitutes a symbolic representation of the contents of this report, and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Ernst + Young LLP

October 3, 2024

Management's Assertion Regarding the Effectiveness of Its Controls Over the S/MIME Certificate Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities – S/MIME, v1.0.3

We, as the management of Google Trust Services LLC and Google Trust Services Europe Limited (collectively, GTS), are responsible for operating the S/MIME Certification Authority (CA) services at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich, Switzerland for the Root and Subordinate CAs in scope for S/MIME Baseline Requirements listed at **Appendix A**.

The management of GTS is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its S/MIME CA business practices disclosure on its website, S/MIME key lifecycle management controls, and S/MIME certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to GTS' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of GTS has assessed the disclosures of its certificate practices and controls over its S/MIME CA services. Based on that assessment, in providing its S/MIME Certification Authority (CA) services at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich Switzerland throughout the period from September 1, 2023, through August 31, 2024, GTS has:

- Disclosed its S/MIME certificate lifecycle management business practices in the applicable versions of GTS' Certification Practice Statement ("CPS") and S/MIME Certificate Policy ("S/MIME CP") as referenced in **Appendix B**, including its commitment to provide S/MIME Certificates in conformity with the applicable CA/Browser Forum Requirements on the GTS website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:

    - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and

    - S/MIME subscriber information is properly authenticated (for the registration activities performed by GTS)

- Maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

for the Root and Subordinate CAs in scope for S/MIME Baseline Requirements at **Appendix A**, based on the *WebTrust Principles and Criteria for Certification Authorities – S/MIME, Version 1.0.3*,

Very truly yours,

GOOGLE TRUST SERVICES LLC &

GOOGLE TRUST SERVICES EUROPE LIMITED

October 3, 2024

Appendix A:

Table 1: Root Cas

Root Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Applicable Notes

CN=GlobalSign
OU=GlobalSign ECC Root CA - R4
O=GlobalSign
	54B07BAD45B8E2407FFB0A6EFBBE33C93CA384D5	0203E57EF53F93FDA50921B2A6	B085D70B964F191A73E4AF0D54AE7A0E07AAFDAF9B71DD0862138AB7325A24A2	

CN=GlobalSign
OU=GlobalSign ECC Root CA - R4
O=GlobalSign
	54B07BAD45B8E2407FFB0A6EFBBE33C93CA384D5	2A38A41C960A04DE42B228A50BE8349802	BEC94911C2955676DB6C0A550986D76E3BA005667C442C9762B4FBB773DE228C	Historical Root CA Certificate

CN=GTS Root R1
O=Google Trust Services LLC
C=US
	E4AF2B26711A2B4827852F52662CEFF08913713E	0203E5936F31B01349886BA217	D947432ABDE7B7FA90FC2E6B59101B1280E0E1C7E4E40FA3C6887FFF57A7F4CF	

CN=GTS Root R1
O=Google Trust Services LLC
C=US
	E4AF2B26711A2B4827852F52662CEFF08913713E	6E47A9C54B470C0DEC33D089B91CF4E1	2A575471E31340BC21581CBD2CF13E158463203ECE94BCF9D3CC196BF09A5472	Historical Root CA Certificate

CN=GTS Root R2
O=Google Trust Services LLC
C=US
	BBFFCA8E239F4F99CADBE268A6A51527171ED90E	0203E5AEC58D04251AAB1125AA	8D25CD97229DBF70356BDA4EB3CC734031E24CF00FAFCFD32DC76EB5841C7EA8	

CN=GTS Root R2
O=Google Trust Services LLC
C=US
	BBFFCA8E239F4F99CADBE268A6A51527171ED90E	6E47A9C65AB3E720C5309A3F6852F26F	C45D7BB08E6D67E62E4235110B564E5F78FD92EF058C840AEA4E6455D7585C60	Historical Root CA Certificate

CN=GTS Root R3
O=Google Trust Services LLC
C=US
	C1F126BAA02DAE8581CFD3F12A12BDB80A67FDBC	0203E5B882EB20F825276D3D66	34D8A73EE208D9BCDB0D956520934B4E40E69482596E8B6F73C8426B010A6F48	

Root Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Applicable Notes

CN=GTS Root R3
O=Google Trust Services LLC
C=US
	C1F126BAA02DAE8581CFD3F12A12BDB80A67FDBC	6E47A9C76CA9732440890F0355DD8D1D	15D5B8774619EA7D54CE1CA6D0B0C403E037A917F131E8A04E1E6B7A71BABCE5	Historical Root CA Certificate

CN=GTS Root R4
O=Google Trust Services LLC
C=US
	804CD6EB74FF4936A3D5D8FCB53EC56AF0941D8C	0203E5C068EF631A9C72905052	349DFA4058C5E263123B398AE795573C4E1313C83FE68F93556CD5E8031B3C7D	

CN=GTS Root R4
O=Google Trust Services LLC
C=US
	804CD6EB74FF4936A3D5D8FCB53EC56AF0941D8C	6E47A9C88B94B6E8BB3B2AD8A2B2C199	71CCA5391F9E794B04802530B363E121DA8A3043BB26662FEA4DCA7FC951A4BD	Historical Root CA Certificate

Table 2: Subordinate CAs

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint

CN=MR1
O=Google Trust Services
C=US
	9A541A6669C30CDA535C16536A13FE620E803FF1	7FF4E5CF7619B94F30F8A47FF8749148	BDF40C618E862D9B6B52718A1FB35BB951DFDBD2428B17D8A3FC64DF9E5DF355

Appendix B

Google Trust Services Certification Practice Statement

Version Number	Effective Date	Note
5.11	7/12/2024	Clarify router and firewall logging requirements
5.10	6/27/2024	S/MIME SMC05 updates + reference section 6.3.2 in certificate profiles from Appendix C
5.9	5/10/2024	SC-70 updates to 1.3.2 and 3.2.2: CAA DNS queries MUST NOT be delegated to third parties.
5.8	3/18/2024	Improve formatting
5.7	2/22/2024	SC-63 & SC-66: Require CRLs and cleanup
5.6	1/12/2024	Remove permission to issue during CAA lookup failure
5.5	12/13/2023	Add 16 newly issued intermediate CAs to section 1.3.1
5.4	12/5/2023	Mention that 4.9.10 only applies to certificates including an OCSP URI
5.3	11/22/2023	Add newly issued LTS32 private CA to section 1.3.1
5.2	11/20/2023	Add newly cross-signed GTS Root R4 to section 1.3.1
5.1	11/10/2023	Minor updates to certificate profiles
5.0	10/11/2023	Add Google Trust Services Europe Ltd
4.21	9/18/2023	Removed revoked Subordinate CA
4.20	9/14/2023	Removed revoked Subordinate CA
4.19	9/13/2023	Removed revoked Subordinate CA

Google Trust Services S/MIME Certificate Policy

Version Number	Effective Date	Note
2.6	8/5/2024	SMC08 update
2.5	7/12/2024	SMC07 update
2.4	6/27/2024	SMIME BR v. 1.0.2 and v. 1.0.3 Updates
2.3	3/18/2024	Improve formatting
2.2	12/5/2023	Make Google policy OIDs optional and mention that 4.9.10 only applies to certificates including an OCSP URI
2.1	11/1/2023	Fix table formatting issues

Version Number	Effective Date	Note
2.0	10/11/2023	Add Google Trust Services Europe Ltd

Appendix C:

**Note: GTS disclosed these incidents as included here for reference but there was no impact on the S/MIME criteria.*

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
1	On February 29, 2024, GTS issued a public statement stating GTS OCSP responders incorrectly responded to requests with an “unauthorized” status for certificates issued by two (2) new intermediate CAs (WE2 and WR2), which impacted 3,301 OCSP responses. GTS' legacy OCSP responder includes an additional pipeline to periodically push status information refreshes for each Sub CA before the status information is propagated. As such, the legacy OCSP responder depends upon the source pipeline to provide the correct information. GTS investigated the issue and determined that the OCSP responders relying on legacy OCSP pipeline were misconfigured for two (2) new intermediate CAs (WE2 and WR2), invalidating any updates received. Thus, the status information was lost, and the responders began returning an “unauthorized” response for the certificates issued under the two impacted CAs. In response to this incident, GTS implemented automation to generate OCSP information for new intermediate CAs, limiting the risk of manual human error, and to ensure their legacy OCSP pipeline is agnostic to intermediate CA addition and removal. GTS also introduced additional monitoring around OCSP and CRLs when a new intermediate CA is configured. The incident was closed in Bugzilla on May 5, 2024, during the current examination period.	**N/A**	Google Trust Services: Incorrect OCSP responses for new ICAs under test (#1882904)

**Note: GTS disclosed these incidents as included here for reference but there was no impact on the S/MIME criteria.*

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
2	On January 25, 2024, GTS issued a public statement stating that the IP validation record for one (1) Alphabet owned IP address was not properly retained during the issuance process, impacting 58 certificates, 12 of which were active at the time of incident discovery. The incident was due to a manual error, as the CAE who approved issuance of the certificate did so without the submission of validation evidence. In response to the incident, GTS implemented technical controls to validate identifiers prior to adding them to validation flat files. The incident was closed in Bugzilla on April 17, 2024, during the current examination period.	**N/A**	Google Trust Services: Failure to properly validate IP address (#1876593)
3	On June 14, 2024, GTS issued a public statement stating that 58 SXG certificates were issued without the presence of "issue" or "issuewild" CAA property. 12 were active at the time the incident was discovered. The incident is limited to SXG-specific CAA validation requirements, and did not impact SSL certificates. All affected certificates complied to the SSL CAA checking requirements. The incident occurred as GTS failed to consider the corner cases where the required "issue" and "issuewild" properties were absent, but other properties were included, leading the CAA validation to succeed where it should have failed. Further, GTS revoked the impacted certificates within 24 hours of discovering the incident. In response to this incident, GTS implemented several new unit tests for SXG CAA, to catch such issues prior to deployment to production. Further, GTS added references within their code to clarify the CAA requirements for future developers and reviewers. The incident was closed in Bugzilla on July 31, 2024, during the current examination period.	**N/A**	Google Trust Services: SXG certificates issued without correctly checking CAA restrictions (#1902670)

**Note: GTS disclosed these incidents as included here for reference but there was no impact on the S/MIME criteria.*

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
4	On June 8, 2023, GTS issued a public statement stating that GTS failed to respond to a Certificate Problem Report (CPR) which requested revocation of a certificate, within 24 hours. GTS investigated the issue and determined that revocation requests sent via the contact form on the website to report CPRs, was no longer passing new requests into pipeline for review. The issue began on 6/4/2023 and impacted four CPR form submissions, one of which was determined to be a valid submission. Per further investigation, it was determined that revocation was not needed since the certificate had been issued to the third-party service provider of the subscriber. As such, no mis-issuances occurred, despite the failure to respond to the valid form submission in 24 hours. In response, the dependent service that caused the issue was fixed on June 9, 2023. To prevent future issues, GTS removed one of the significant dependencies of the CPR revocation request process and added checks to ensure that CPRs are responded to within the required 24-hour time frame. Furthermore, CPR visibility among the team was increased via additional notification mechanisms to avoid bottlenecks and improve response times. The incident was closed within the current examination period on November 2, 2024 due to open community discussion requesting more specific information on how GTS is updating their CPR process. This incident did not impact any CPRs during the current examination period.	**N/A**	Google Trust Services: Failure to respond to CPR within 24 hours (#1837519)